Critical Infrastructure Security

Lecture 2

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

Administrative

Deadline - 16th Feb 2022

Papers	Presentation	Opponent	Defender
	Student Name (Roll No.)	Student Name (Roll No.)	Student Name (Roll No.)
Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective	Hamda Tehami(220283)		
Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.	Shajeera Tehami(220284)		
Cyber-security on smart grid: Threats and potential solutions	Hamda Tehami(220283)		
RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid			
Lest We Remember: Cold Boot Attacks on Encryption Keys	M. Bilal Rasool (220337)		
Light commands: laser-based audio injection attacks on voice-controllable systems	M. Bilal Rasool (220337)		
What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices	Shajeera Tehami(220284)		
Adversarial Attacks against LiDAR Semantic Segmentation in Autonomous Driving			

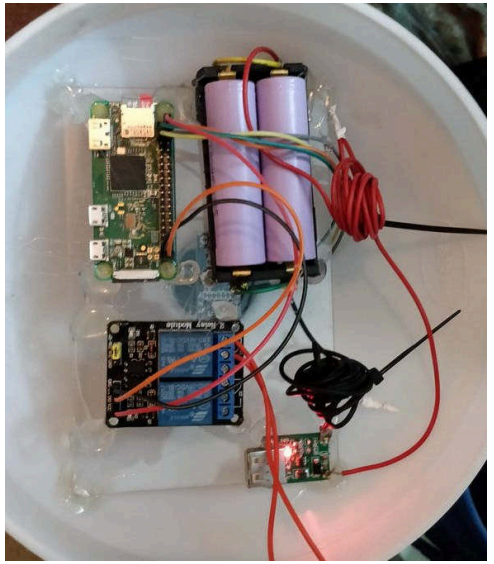
Before going into Cyber Security Concepts

Industrial Control Systems

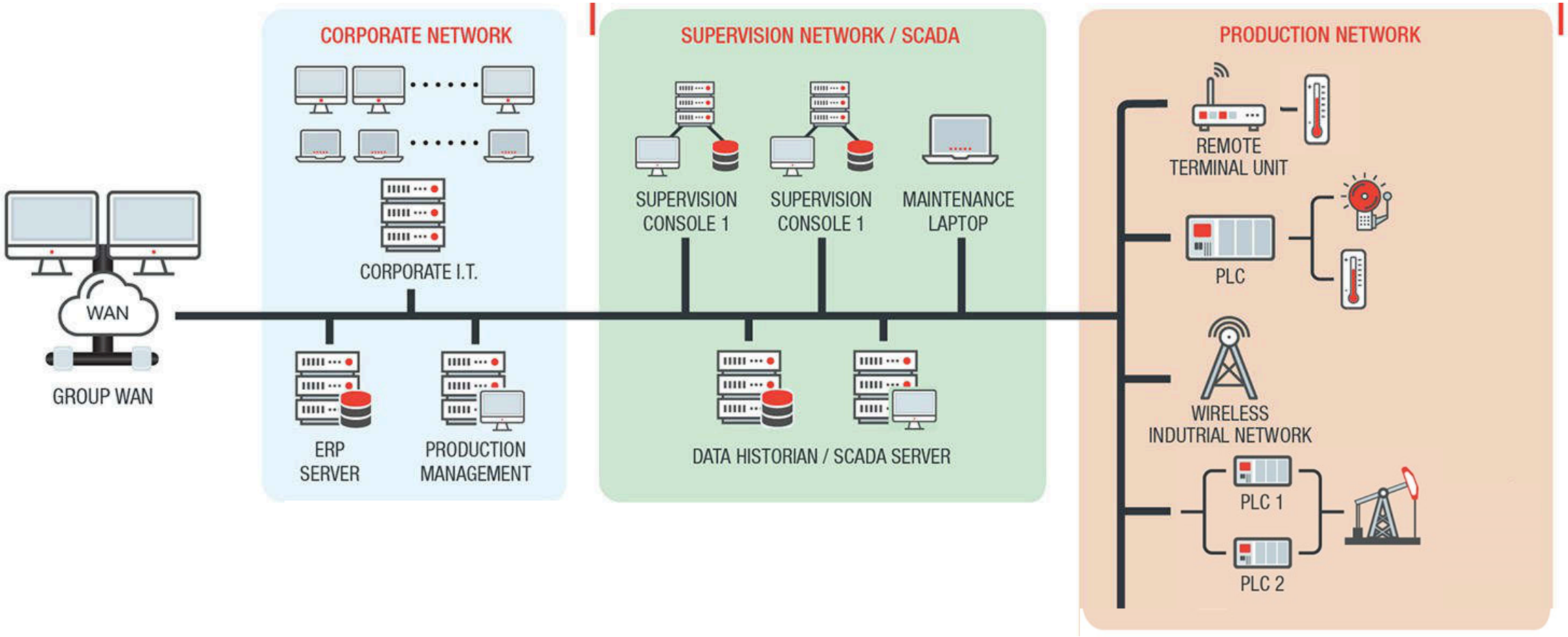
- Components of ICS
- Types of ICS
- Wireless infrastructure in ICS

Introduction

- As the name suggests, an ICS is a system for **controlling some industrial processes**
- ‘Industrial’ suggests we’re talking about **huge factories**, but it may even be a simple water tank level controller
- Since the ‘attack’ on an ICS may target any of its components therefore we discuss the common elements of an ICS

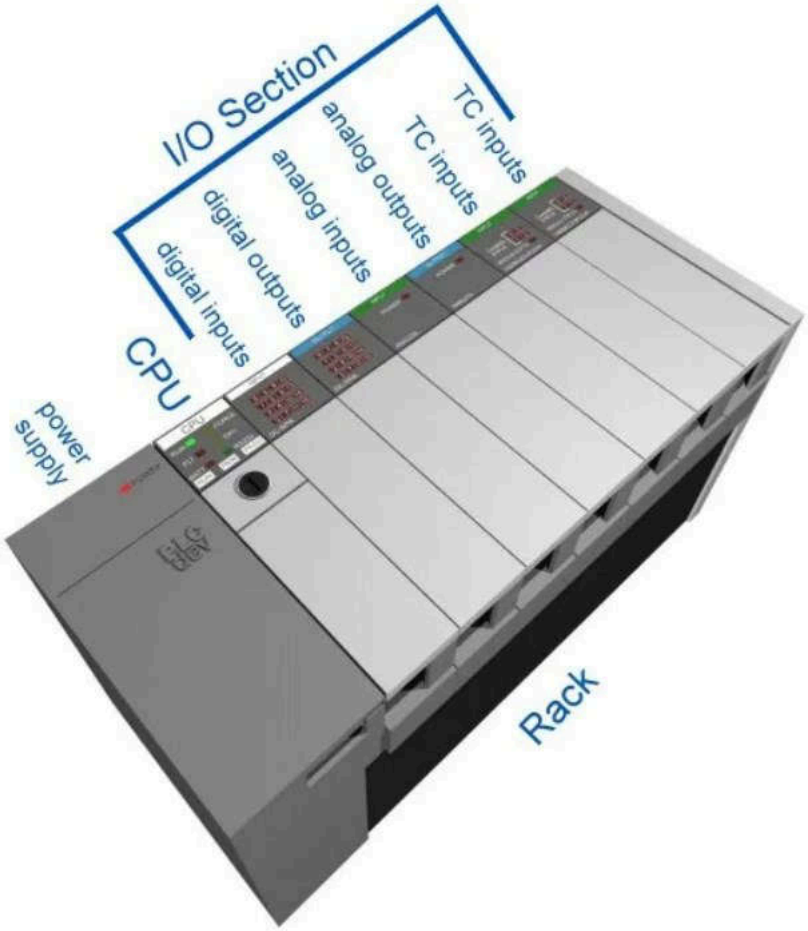


ICS – Complete Picture



Components of ICS

- **Programmable Logic Controllers (PLCs)**
  - It all began with discrete logic components (AND gates, OR gates, etc.)
  - Now PLCs are microprocessor based devices
  - Contains CPU, I/O modules, communication interface
  - Reads inputs (digital or analog) from sensors, and receives commands from the main controller
  - Performs actions (by changing digital outputs) as per the process control logic
  - Placed at the boundary of cyber world and physical world
  - Runs a real-time operating system with very tight timing constraints



Components of ICS

- **Remote Terminal Units (RTUs)**
  - Normally mounted in remote locations
  - Typically used in harsh environmental conditions
  - Normally no reliable continuous power supply available at the locations where they are installed, thus frequently requiring small solar panels and batteries to provide electricity.
  - Can be categorized as:
    - Field RTU
      - Receives sensor data from the field
      - Acts as per programmed logic
    - Station RTU
      - Connects to various field RTUs as supervisor
      - May also receive commands from main controller

Components of ICS

- **Remote Terminal Units (RTUs)**

Image courtesy Lucy Electric Limited

Components of ICS

- **Intelligent Electronic Device (IED)**
  - Focused on power generation / distribution systems
  - Performs protection, monitoring, control, metering and communication functions
  - Typical use case is ‘circuit breaker’ action – connecting or disconnecting power systems as per the status of specific inputs and process logic

Components of ICS

- **Intelligent Electronic Device (IED)**

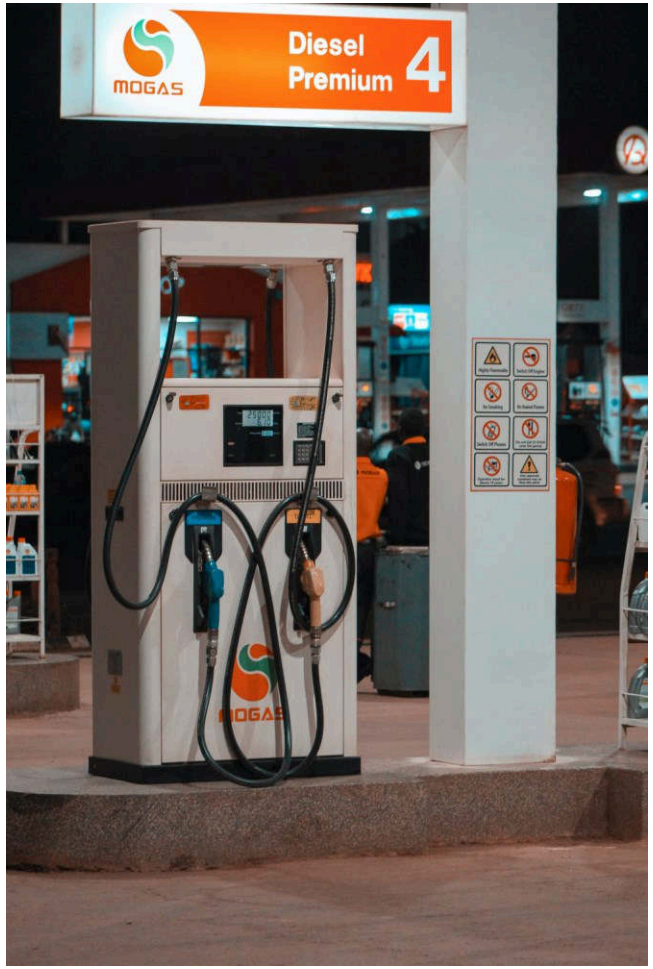
Image courtesy Schweitzer Engineering Laboratories

Components of ICS

- **Engineering workstation**
  - Just a PC or server running common OS (Windows or Linux)
  - Hosts the development environment for programming and configuring the controllers (PLCs, RTUs, IEDs)
  - Not usually involved in live process automation and control. Why?

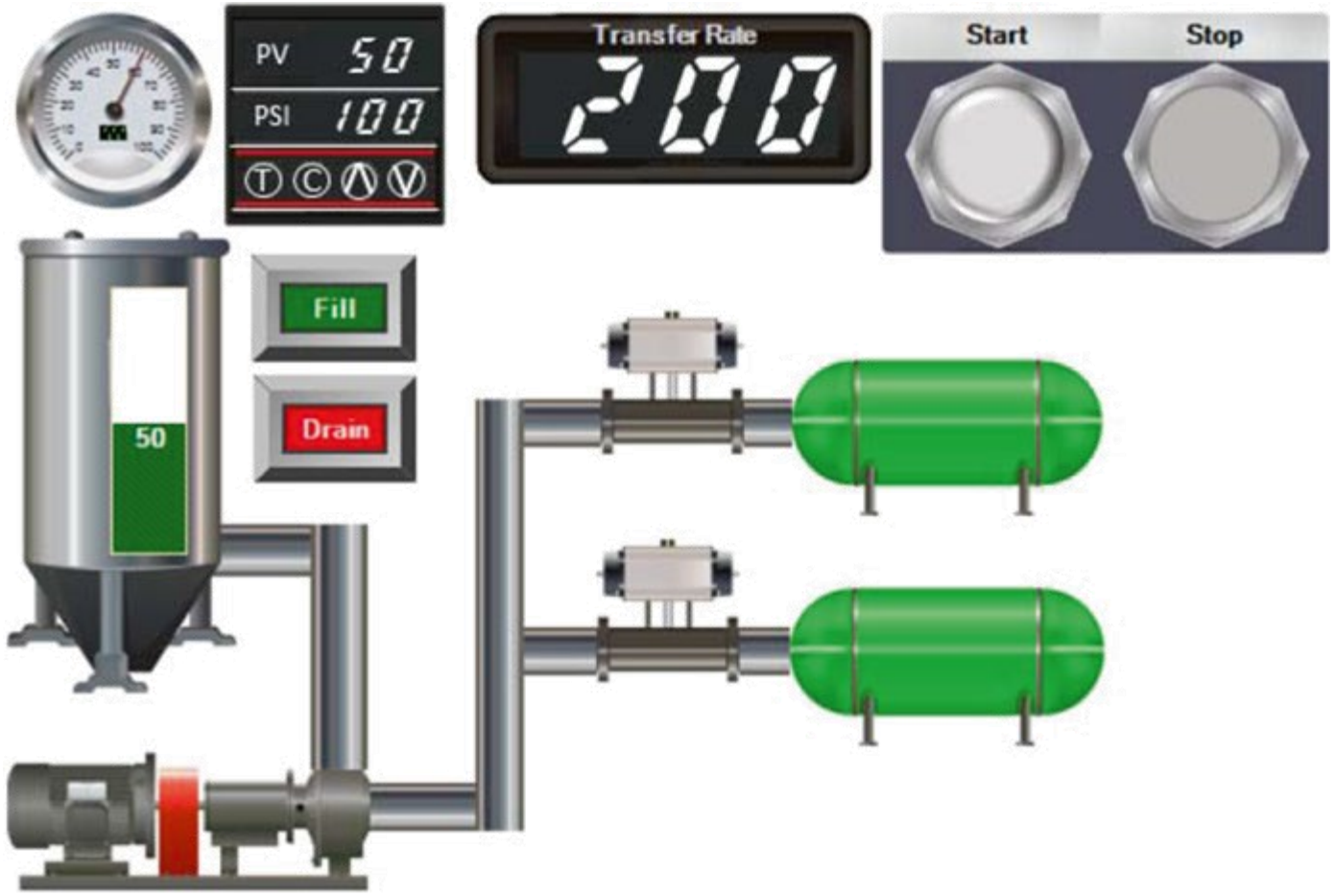
Components of ICS

- **Human Machine Interface (HMI)**
  - It’s self explanatory!
  - Displays process status to the human operator
  - Takes commands from the operator and sends to the controller
  - The touchscreen you see on CNG pumps and petrol stations are examples of HMI
  - HMI can be software based
    - Installed on PCs, tablets, mobile phones
  - Or hardware based
    - Specific devices that connect directly with the controller



Components of ICS

- Human Machine Interface (HMI)



Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

Components of ICS

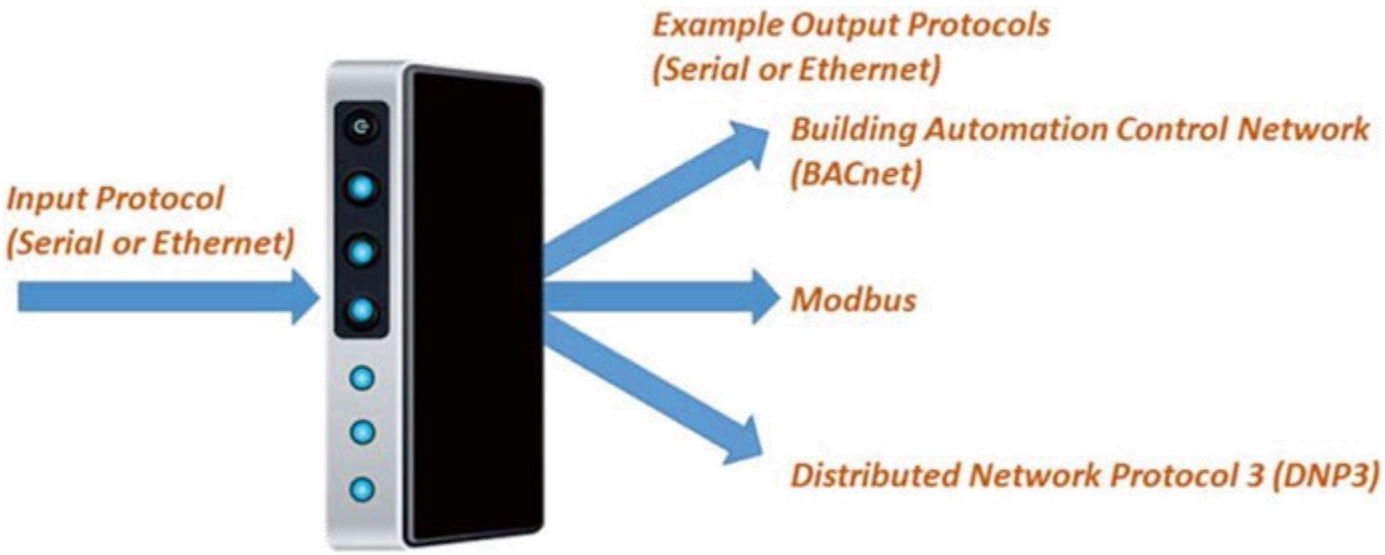
- **Data Historian**
  - Process values are not only shown on the HMI…
  - … these also need to be stored (logged) for later analysis
  - Data historian is a software for logging live process data into a database
  - Data points are time-stamped so that sequence of events can be recreated during off-line analysis

Components of ICS

- **Communications gateway**
  - Works as an ‘adapter’
  - Generally used to interconnect devices with different communications protocols
  - Typical use case involves communicating between two different ‘zones’

Components of ICS

- Communications gateway



Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

Components of ICS

- Field devices
  - Elements that interact directly with the ‘real’ world
  - Convert physical properties into electronic signals (digital or analog) and vice-versa
  - Typical devices include:
    - Sensors
    - Transducers
    - Actuators
    - Machinery

Components of ICS

- Field devices

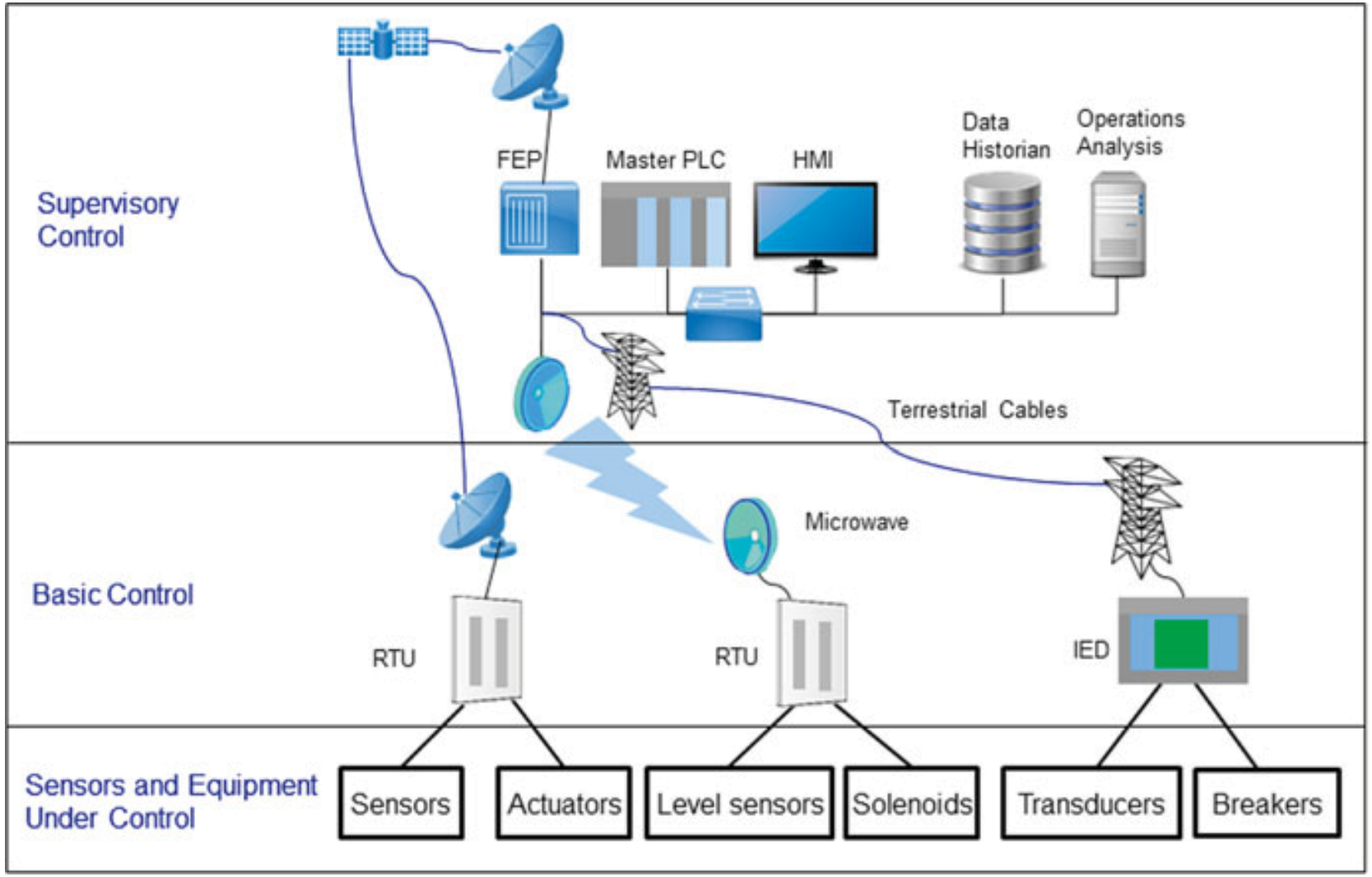
Voltage Transducer

Stepper Motor and Driver

Valve and Motorized Drive

Image courtesy Aim Dynamic (www.aimdynamics.com) and Advanced Micro Controls, Inc.

Components of ICS



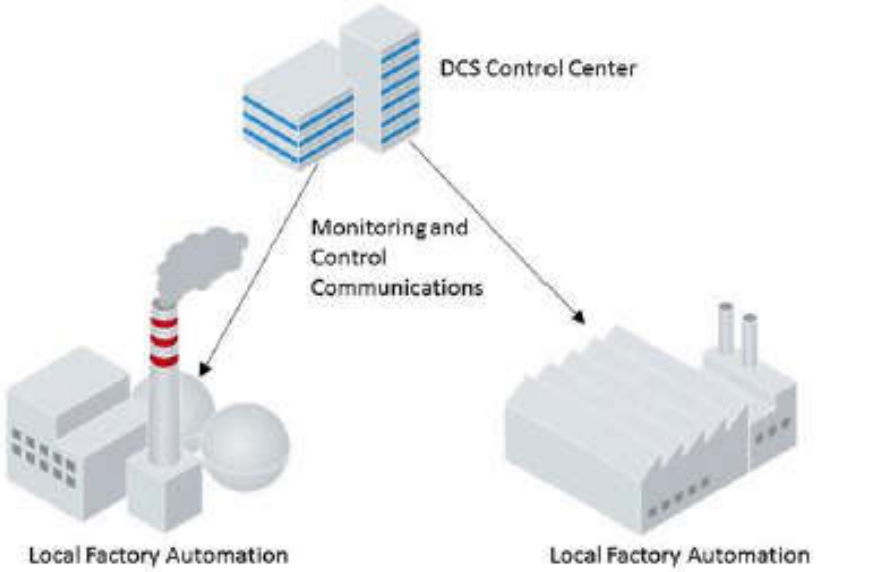
Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

Types of ICS

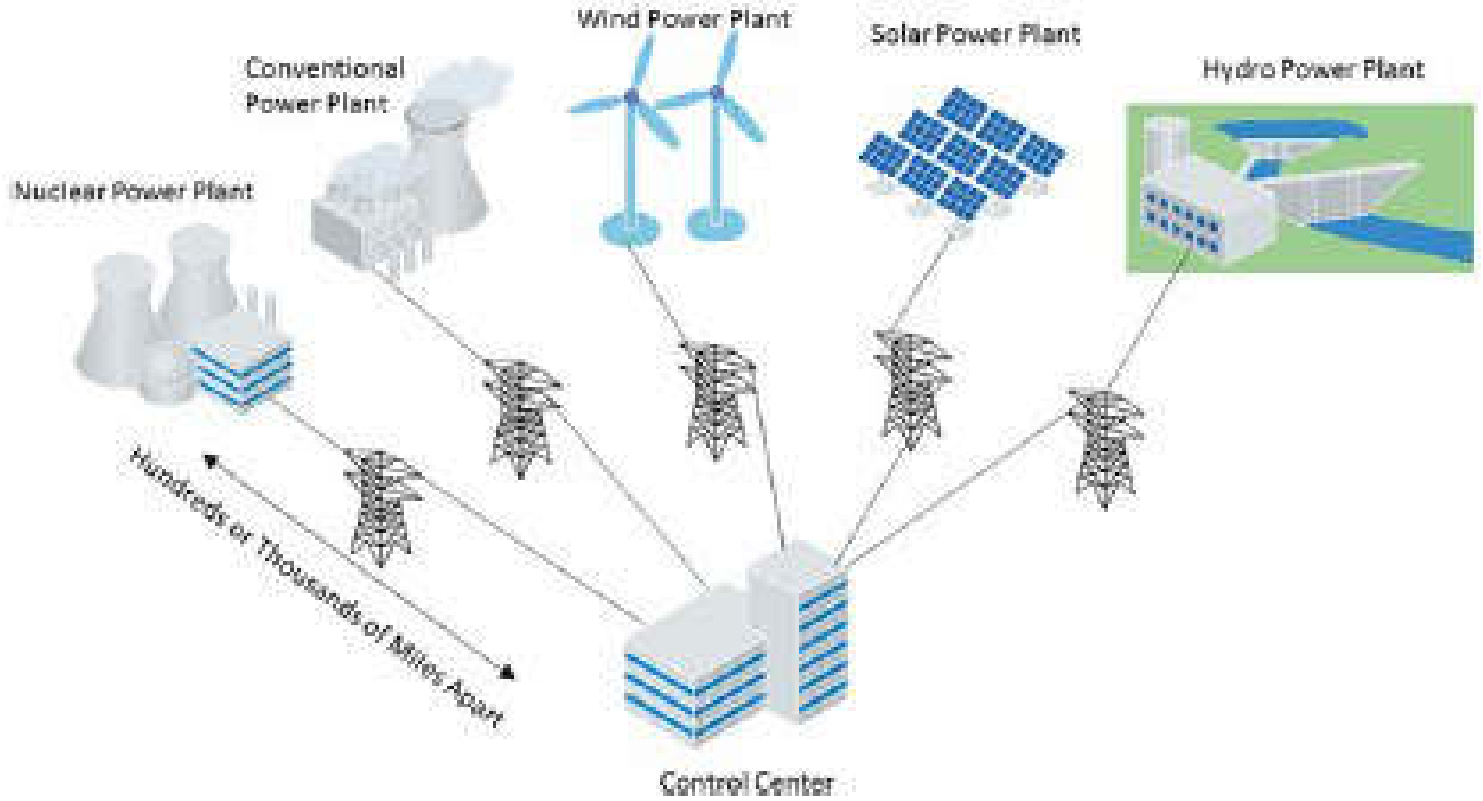
- ICSs can be categorized on the basis of their application areas, such as:
- **Process Control Systems**
  - Typically used in the industry for automation of manufacturing processes
- **Safety Instrumented Systems**
  - Works in parallel with the PCS
  - Monitors the automation process from safety aspects
  - Implements interlocking mechanisms to prevent unwanted and unsafe process state
- **Distributed Control Systems**
  - A Distributed Control System (DCS) controls multiple automation processes at a single site

Types of ICS

- **Building Automation Systems**
  - Monitors and controls a building's infrastructure services such as electricity, gas, water, HVAC, fire protection, security
- **SCADA Systems**
  - Supervisory Control And Data Acquisition systems are used to monitor and control operations in geographically distant facilities
  - SCADA control center may receive input from multiple RTUs or PLCs, thousands of miles away using different communication protocols
  - A SCADA system may be composed of multiple PCSs


DCS Control Center
Monitoring and
Control
Communications
Local Factory Automation
Local Factory Automation

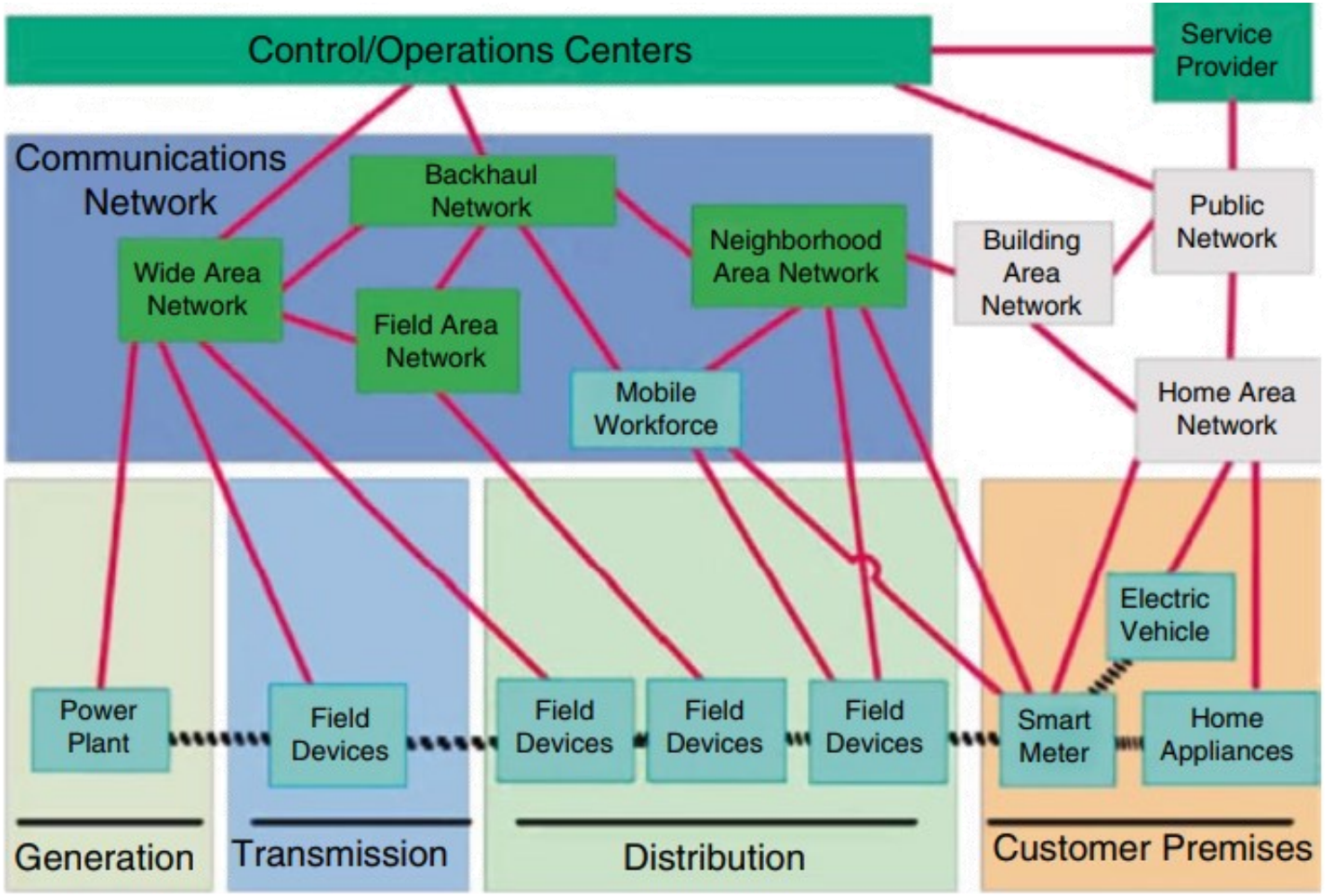

Smoke Detectors
Air Conditioning
Surveillance
Security
Water
Smart Thermostat
Power & Energy


Wind Power Plant
Solar Power Plant
Hydro Power Plant
Conventional
Power Plant
Nuclear Power Plant
Hundreds or Thousands of Miles Apart
Control Center

Wireless infrastructure in ICS

- What are the advantages of wireless communication over wired one?
- What are the challenges in using wireless communication?

Wireless infrastructure in ICS



An example ICS communication architecture (e.g., smart grid)

Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

Wireless infrastructure in ICS

- Could be divided into three categories:
  - Short range
    - Within the building
      - Bluetooth, Zigbee, Z-Wave, Wi-Fi
  - Medium range
    - From one building to the next
      - Zigbee, WirelessHART
  - Long range
    - From one premises to the other
      - UWB, Microwave, Satellite!

Case study: The Bhopal Disaster

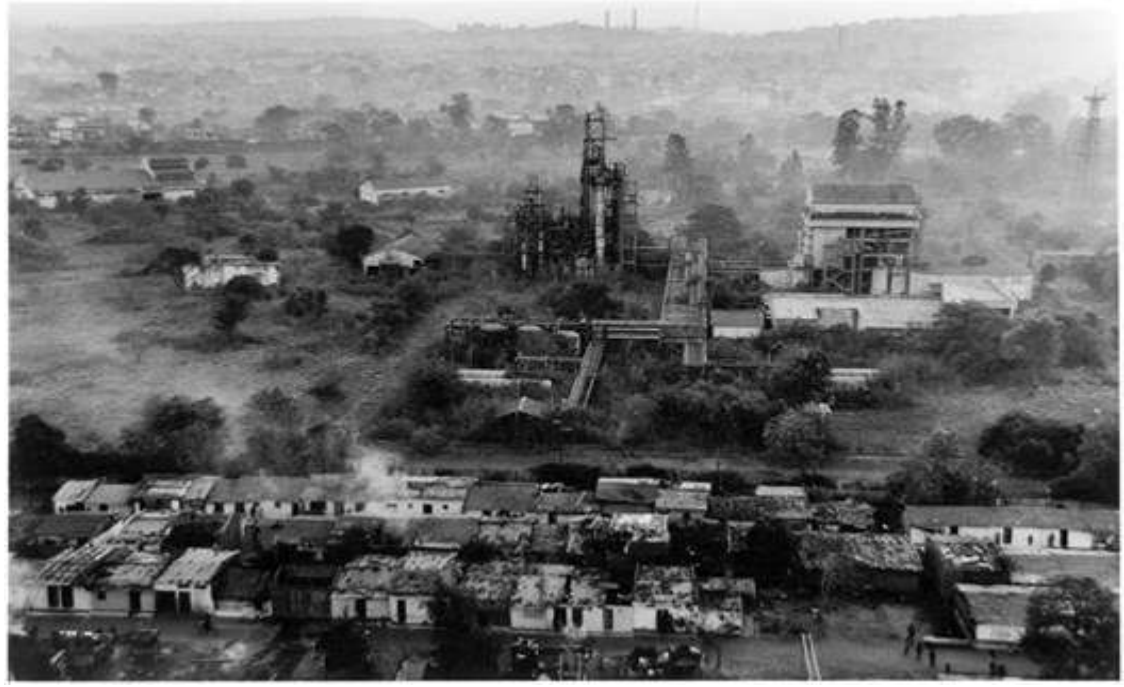
- Toxic gas leak at the Union Carbide India Limited (UCIL) pesticide plant in Bhopal, India

- On a night in early **December, 1984**, a malfunction in some pipes allowed water to enter one of the MIC holding tanks

- Chemical reaction and increased pressure in the tank

- Emergency venting system engaged, releasing around 30 tons of a dangerous mix of MIC gas

- **4,000 people died**



Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over